Lacework provides runtime threat defense that enables security teams to identify vulnerabilities across the entire scope of their cloud and containerized environments. This includes identifying security issues with serverless resources, applications, networks, file systems, APIs, processes, and other elements that could increase the threat vector of an organization’s infrastructure.

At Lacework, we developed our end-to-end security solution from the ground up, specifically for the rapidly changing cloud. Our platform provides a comprehensive solution that encompasses cloud configurations, account activities, workload/runtime analysis, and automated anomaly and threat detection.

With an emphasis on events happening at runtime, organizations can identify issues before they spread within their cloud or container environment.
IDENTIFYING RISKS AT RUNTIME

By identifying risks in runtime, enterprises get better intelligence about threats coming from within the organization’s own walls, both for actual internal resources and for interactions with third-party data and applications. Lacework identifies and analyzes things like dead accounts, inappropriate data exfiltration, and other aspects of misuse within a cloud or container environment to identify issues.

Lacework’s approach uses automation and unsupervised machine learning. Security teams are able to deploy the Lacework agent across multiple cloud platforms, within application orchestration environments like Docker and Kubernetes, and even in hybrid workloads. As an SaaS service, organizations are able to review historical event data across their infrastructure to understand where breaches occurred and identify risk areas.

In a rapidly changing deployment environment, traditional security rules are stale as soon as they are deployed and new attacks are missed because they require someone to write the appropriate rule. Lacework’s automated approach provides the following benefits:

1.) **No Missed Events:** Lacework will always alert you on new activity, so that you are given a chance to investigate any behavior within your environment that could potentially be malicious.

2.) **Low Alert Noise:** Lacework will only alert you on what is new or anomalous, preventing alert fatigue within your organization.

3.) **Simple Operations & Maintenance:** Automated workload detection means no writing and maintaining error prone rules. With Lacework you will not need to constantly maintain rules, allowing you to focus on securing your environment.
THE POWER OF POLYGRAPH

Lacework’s foundation is Polygraph, a deep temporal baseline, which we present to users as a set of behavioral maps or “Polygraphs.” With the complexity and volume of a modern data center, Polygraph employs a baseline, zero-touch approach without leaving any blank spaces where attackers can hide.

CLOUD SECURITY, AT SCALE, AT THE SPEED OF BUSINESS

The modern cloud infrastructure allows organizations to deploy, scale, and configure their infrastructure faster than ever. The ability to automate and operate at DevOps speed poses a challenge to traditional security approaches. Lacework’s approach is to automate the detection of threats and anomalies and provide human understandable investigative insights. Lacework supports public clouds AWS, GCP, Azure and supports computer hosts and containers.
SECURITY VISIBILITY
Get deep observability into your cloud accounts, workloads, and microservices to give you tighter security control.

THREAT DETECTION
Identify common threats that specifically target your cloud servers, containers, and IaaS accounts so you can action on them before your company is at risk.

ANOMALY DETECTION
Detect and resolve anomalous changes in behavior across your workloads, containers, and IaaS accounts that represent a security risk or an IOC.

HOST COMPLIANCE
Achieve compliance for SOC 2, PCI DSS, HIPAA, and other compliance measures that require host intrusion detection (HIDS).

CONFIGURATION COMPLIANCE
Spot IaaS account configurations that violate compliance & security best practices the could put your company at risk.